UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/071,228	02/08/2002	Steven A. Pettit	ENB-012RCE2	9237

86738 7590 10/30/2009

MCCARTER & ENGLISH, LLP BOSTON
265 Franklin Street
Boston, MA 02110

EXAMINER	
WONG, WARNER	
ART UNIT	PAPER NUMBER
2471	
MAIL DATE	DELIVERY MODE
10/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/071,228	PETTIT ET AL.	
	Examiner	Art Unit	
	WARNER WONG	2471	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-9,11,13-15,17,19-21,23,26-29,31,33-35,37 and 40-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,13-15,17,26-29,31,33-35,37,40 and 41* is/are rejected.

7)☒ Claim(s) *7-9,11,19-21,23 and 42-50* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-3, 5, 13-15, 17, 33-35, 37 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over See (US 2003/0021283) in view of Moriconi (US 6,158,010).

Regarding claim 1, See describes a distributed network management system of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

creating, with a relationship management module, one or more packet rules (policy rules) for analyzing packets received at one or more network devices of the communications network, each rule including a condition and action to be taken as part of providing a service of the communication network if a packet received at a device satisfies the condition, wherein one or more packet rules are defined to examine any portion of a packet (fig. 2 & 4 and para. 35 & 38, policy console 20 (relationship management module) accessing policy repository for translating the network address (portion of packet) upon satisfaction of 1+ conditions);

storing the one or more packet rules in the communications network (fig. 2 & para, 35, policy rules stored in repository table of repository 20 as part of the network);

creating, with the relationship management module (fig. 2, policy console 20), one or more service abstractions (policy groups), each service abstraction representing a communication network service to be provided to users of the communication network, each service abstraction including a [named] set of one or more of the packet rules, that in combination provide the represented communication network service (para. 35, "According to one embodiment, certain policy rules (in combination) are organized into policy groups (service abstractions) based on a rule type 52". Policy groups comprising policy rules are used for (represented communication network service) network devices, where a network device may be computer hosts (user), para. 27);

storing the one or more service abstractions (para. 35, policy groups stored in repository table);

host of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

See fails to describe:

associating, with the relationship management module, one or more of the service abstractions with the identity of the authenticated user of the communication network;

in response to receipt of a packet at any of the network devices from the authenticated user, using, by any of the network devices, the one or more service

abstractions associated with the identity of the authenticated user to control usage of network resources on the communication network, the using including applying the packet rules in the one or more service abstraction to the packet.

Moriconi describes a service allocation method, suggesting:

associating one or more of the service abstractions with the identity of the authenticated user of the communication network (col. 6, lines 20-30, policy generalized in groups and hierarchies (service abstractions) are used to specify (associate) access of users (identity of authenticated user) in the system environment (network));

in response to receipt of a packet at any of the network devices from the authenticated user, using, by any of the network devices, the one or more service abstractions (col. 6, lines 29-30 in view of col. 4, lines 26-30, hierarchically layered policies are distributed to clients or server (any network device) to handle a user's authorization request (receipt of packet).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer).

The motivation for combining the teachings is that this greatly improves manageability & lead to more comprehensible policies (Moriconi, col. 6, lines 30-32).

Regarding claim 2, See and Moriconi combined further describe:

configuring a network device of the communication network with one or more packet rules according to at least one of the service abstraction (Moriconi, col. 4, lines

26-30 & col. 6, lines 29-30, the hierarchically layered policies (rules according to service abstraction) is configured to a server or client (network device)).

Regarding claim 3, See already describes logic to configure a port module network device of the communications network with one or more packet rules (para. 22, network policies (packet rules) are used to disable network ports (modules)).

See and Gray combined further suggest:

the packet rules are according to one of the role abstraction (Moriconi, col. 6, lines 29-30, policies (rules) are according to hierarchically layer (role abstraction)).

Regarding claim 5, See and Moriconi combined further describes:

distributing the one or more service abstractions to one or more network devices residing on the communications network (Moriconi, col. 4, lines 26-30 & col. 6, lines 29-30, the hierarchically layered policies (service abstraction) is distributed to a server or client (network device) in the computing environment of fig. 1, communications network).

Regarding claim 13, See describes a system of controlling usage of network resources (network manager) on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

a rule editing module enabling the network manager (fig. 2, policy console) to edit one or more packet rules for analyzing packets received at one or more devices of the communication network (fig. 4 and para. 35 & 38, functionality (rule editing module) for creating (editing) rules for translating (analyzing) the network address of packets);

storage means for storing the packet rules (para, 35, policy rules stored in repository table);

See fails to describe:

a service editing module enabling the network manager to edit one or more service abstractions, each service abstraction representing a communication network service to be provided to users of the communications network, each service abstraction including a named set of one or more of the packet rules that, in combination, provide the represented communications network service;

a user management module enabling the network manager to associate users of the communications network with one or more of the service abstractions.

Moriconi describes a service allocation method, suggesting:

a service editing module enabling the network manager to edit one or more service abstractions, each service abstraction representing a communication network service to be provided to users of the communications network, each service abstraction including a named set of one or more of the packet rules that, in combination, provide the represented communications network service (fig. 8 & col. 6, lines 29-30, manage policy process (service editing module) manages (edits) the tree representing the hierarchically layered policies (service abstraction) for service comprising identifiable groups (named sets) of policies (rules) for users);

a user management module enabling the network manager to associate users of the communications network with one or more of the service abstractions (fig. 4 & col. 11, lines 28-34, logger 216 (user management module) enables policy manager to audit

logged requests of clients (users) on its hierarchically layered policies (service abstraction)).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer).

The motivation for combining the teachings is that this greatly improves manageability & lead to more comprehensible policies (Moriconi, col. 6, lines 30-32).

Regarding claim 14, See and Moriconi combined further describe:

configuring a network device of the communication network with one or more packet rules according to at least one of the service abstraction (Moriconi, col. 4, lines 26-30 & col. 6, lines 29-30, the hierarchically layered policies (rules according to service abstraction) is configured to a server or client (network device)).

Regarding claim 15, See already describes logic to configure a port module network device of the communications network with one or more packet rules (para. 22, network policies (packet rules) are used to disable network ports (modules)).

See and Moriconi combined further suggest:

the packet rules are according to one of the role abstraction (Moriconi, col. 6, lines 29-30, policies (rules) are according to hierarchically layer (role abstraction)).

Regarding claim 17, See and Moriconi combined further describes:

distributing the one or more service abstractions to one or more network devices residing on the communications network ((Moriconi, col. 4, lines 26-30 & col. 6, lines 29-30, the hierarchically layered policies (service abstraction) is distributed to a server or

client (network device) in the computing environment of fig. 1, communications network).

Regarding claim 33, See describes a system of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

a rule editing module to create one or more packet rules for analyzing packets received at one or more devices of the communication network (para. 35, function (rule editing module) which create policy (packet) rules), each rule including a condition and action to be taken if a packet received at a device satisfies the condition, wherein the one or more packet rules are defined to examine any portion of a packet (fig. 4 and para. 35 & 38, for translating the network address (portion of packet) upon satisfaction of 1+ conditions);

storage means for storing one or more created role abstractions or one or more created packet rules (para. 53, repository table storing the policy (packet) rules).

See fails to describe:

a role editing module to create, in response to a user, one or more role abstractions associated with an authenticated user, each role abstraction representing a role of an authentication user with respect to the communication network for controlling usage of network resources on the communications network by the authenticated user and each role abstraction including a set of one or more packet rules.

Moriconi describes a multilevel service abstraction (fig. 1), comprising:

a role editing module to create, in response to a user, one or more role abstractions associated with an authenticated user, each role abstraction representing a role of an authentication user with respect to the communication network for controlling usage of network resources on the communications network by the authenticated user, and each role abstraction including a set of one or more packet rules (fig. 8 & col. 6, lines 29-30, manage policy process (role editing module) manages (edits) the tree representing the hierarchically layered policies (service abstraction) for service comprising identifiable groups of policies (rules) for users);

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer).

The motivation for combining the teachings is that this greatly improves manageability & lead to more comprehensible policies (Moriconi, col. 6, lines 30-32).

Regarding claim 34, See already describes logic to configure a port module network device of the communications network with one or more packet rules (para. 22, network policies (packet rules) are used to disable network ports (modules)).

See and Moriconi combined further suggest:

See and Moriconi combined further describe:

the packet rules are according to one of the role abstraction (Moriconi, col. 6, lines 29-30).

Regarding claim 35, See already describes: port configuration logic to configure a port module of a switching device with one or more packet rules (para. 22, network policies (packet rules) are used to disable network ports).

See and Moriconi combined further describe:

the packet rules are according to one of the role abstraction (Moriconi, col. 6, lines 29-30).

Regarding claim 37, See and Moriconi combined further suggest:

a distribution module to distribute one or more role abstractions to one or more network devices residing on the communications network (Moriconi, col. 4, lines 26-30 & col. 6, lines 29-30, the hierarchically layered policies (role abstraction) is distributed to a server or client (network device) in the computing environment of fig. 1, communications network).

Regarding claim 40, See describes a method of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

creating one or more packet rules (para. 35, policy rules) for analyzing packets received at one or more devices of the communication network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition, wherein the one or more packet rules are defined to examine any portion of a packet (fig. 4 and para. 35 & 38, for translating the network address (portion of packet) upon satisfaction of 1+ conditions);

storage means for storing one or more created packet rules (para. 53, repository table storing the policy (packet) rules);

See lacks describing:

a computer program product to perform the above-mentioned system, comprising a computer readable medium and computer readable signals stored on the computer readable medium that define instructions that, as a result of being executed by a computer, instruct the computer to perform the process.

in response to a user, creating one or more role abstractions associated with an authenticated user each role abstraction representing a role of a user with respect to the communications network, and each role abstraction including a set of one more packet rules.

Moriconi describes:

a computer program product to perform the above-mentioned system (col. 17, lines 37-39), comprising a computer readable medium and computer readable signals stored on the computer readable medium that define instructions that, as a result of being executed by a computer, instruct the computer to perform the process:

in response to a user, creating one or more role abstractions associated with an authenticated user each role abstraction representing a role of a user with respect to the communications network, and each role abstraction including a set of one more packet rules (role abstractions of rules) to handle a user's authorization request (receipt of packet).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer).

The motivation for combining the teachings is that this greatly improves manageability & lead to more comprehensible policies (Moriconi, col. 6, lines 30-32).

Regarding claim 41, See and Moriconi combined further describe:

The relationship management module comprises electronic circuitry (See, fig. 3, network device is electronic circuitry).

Claim 26 is a computer readable medium claim where its limitations are all described in method claim 1. Hence, it is rejected under the same rationale.

Claims 27-29 & 31 are method claims which comprise limitations of system claims 33-35 & 37 respectfully. Hence, they are rejected under the same rationale.

Allowable Subject Matter

2. **Claims 7-9, 11 and 19-21 and 23** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 42-50 allowed.

Response to Arguments

3. Applicant's arguments with respect to claims 1-3, 5, 13-15, 17, 26-29, 31, 33-35, 37 and 40 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Weisser (US 2002/0087671) describing mapping between customer identity and network elements with abstraction layers, Muftic (US 5,745,574) describing security services for applications and users, and Leppek (US 5,787,177) describing integrated network security access control system for users.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WARNER WONG whose telephone number is (571)272-8197. The examiner can normally be reached on 6:30AM - 3:00PM, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chi Pham can be reached on (571) 272-3179. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Warner Wong
Examiner
Art Unit 2471

/Warner Wong/
Examiner, Art Unit 2471